



CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

Practical Cybersecurity for Open Science Projects

The need for cybersecurity in science projects (at any scale) and first steps

Craig Jackson, Chief Policy Analyst, CACR and Co-PI, CTSC
Susan Sons, Senior Security Analyst, CACR and CTSC

Contributors:

Bob Cowles, CACR / CTSC / Brightlite Information Security
Von Welch, Director, CACR and PI, CTSC

Indiana University
27 April 2016

trustedci.org/trainingmaterials

Center for Trustworthy Scientific Cyberinfrastructure

The NSF Cybersecurity Center of Excellence

CTSC's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.



Outline

1. Introduction: Audience, Goals, Caveats, Terminology
2. Cybersecurity & Science
3. Cybersecurity Programs
4. Programmatic Must-Do's (at any size/complexity)

-1- Introduction

The audience for today's session

CTSC's work spans the full range of NSF-funded projects and facilities.

Today, we're focused on smaller science projects...

- Unlikely to have dedicated security personnel or funding
- Unlikely to need tons of policy and process
- Relationships (e.g., with home institution) are particularly important
- But, can still be working with highly valuable, sensitive data and IT infrastructure.

Goals of this session

Provide you:

1. A sense of cybersecurity's relevance to science projects.
2. A sense of the complexity and scope of cybersecurity.
3. A sense of how cybersecurity programs can help you cope with that complexity (and protect your science).
4. A few “must-do” action items that are truly do-able and truly important.

And:

5. Get your questions on the table.

Caveats & Terminology

The views and conclusions contained herein are those of the author(s) and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the National Science Foundation or Indiana University.

Note on Terminology: We may use terms that have very specific meaning at IU; if so, we are using those terms generally and are **not** referring to IU's definitions.

e.g., “Sensitive data” – <https://kb.iu.edu/d/augs>

Some more notes about terminology

1. We use “**information security**” and “**cybersecurity**” more or less interchangeably. We often prefer the former, but have gotten trapped in the cybereverything.
2. If we throw out a **term that you don't understand, please stop us!**

-2-

Cybersecurity & Science

Our information technology world is **stormy**

Anthem

Home FAQ A Letter from our CEO En Español

How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me in It

CNBC

HOME U.S. NEWS MARKETS INVESTING TECH SMALL BUSINESS

HACKING AMERICA

FBI: Computer expert briefly made plane fly sideways

Nasa hack: AnonSec attempts to crash \$222m drone, releases secret flight videos and employee data

By Mary-Ann Russon

February 1, 2016 13:05 GMT

f 2,127 t g+ e

PENNSTATE

PENN S

search Academics Impact Ca

College of Engineer
network disabled i
o sophisticated cy

engadget

Thirty Meter Telescope's website was hacked to protest its construction

by Mariella Moon | @mariella_moon | April 28th 2015 At 4

t f g+ e



The Washington Post

PM databases
sed 22.1 million people,
thorities say

Digital subscriptions
SUBSCRIBE

Symantec Security

Symantec Official Blog

Digital Extortion Rise

By: Roger Park SYMANTEC EMPLOYEE

Created 20 Apr 2015

engadget

Old Intel chips are vulnerable to a fresh security exploit

by Jon Fingas | @jonfingas | August 8th 2015 At 10:11pm

t f g+ e



Science must be trustworthy and reproducible



"BLIND INJECTION" STRESS-TESTS LIGO AND VIRGO'S SEARCH FOR GRAVITATIONAL WAVES

The LIGO Scientific Collaboration and the Virgo Collaboration completed an end-to-end system test of detection capabilities at their recent joint collaboration meeting in Arcadia, CA. Analysis of data from LIGO's most recent observation run revealed evidence of the elusive signal from a neutron star spiral black hole. The collaboration knew that the "detection" could be a "blind injection" – a fake signal added under the assumption that the signal was real, and wrote and approved a scientific paper reporting the breaking discovery. A few moments later, according to plan, it was revealed that the signal was indeed injection.

While the scientists were disappointed that the discovery was not real, the success of the analysis was compelling demonstration of the collaboration's readiness to detect gravitational waves. LIGO and Virgo scientists are looking forward to observations with the advanced detectors which are expected to continue.



nature
International weekly journal of science

Home | News & Comment | Research | Careers & Jobs | Current Issue | Archive | Audio & Video | For Authors

News & Comment | News | 2016 | February | Article

Biotech giant publishes failures to confirm high-profile science

Amgen posts three studies at new online channel for discussing reproducibility.

Mona Baker

04 February 2016

Rights & Permissions

A biotechnology firm is releasing data on three failed efforts to confirm findings in high-profile scientific journals — details that the industry usually keeps secret.

Amgen, headquartered in Thousand Oaks, California, says that it hopes the move will encourage others in industry and academia to describe their own replication attempts, and thus help the scientific community to get to the bottom of work that other labs are having trouble verifying.

The data are posted online at a newly launched channel dedicated to quickly publishing efforts to confirm scientific findings. The 'Preclinical Reproducibility and Robustness' channel is hosted by *F1000Research*, the publishing platform of London-based publishers Faculty of 1000 (F1000). Scientists who are concerned about the irreproducibility of preclinical research say that they welcome the initiative — but are not sure whether it will gain traction.



Understanding Science
how science really works

Home | Glossary | Home

Understand the Science | For Teachers | Resources Library

The science checklist applied: Cold fusion

Fusion occurs when two light atoms, like hydrogen, join together, or fuse, into a single heavier atom, releasing a lot of energy in the process. In 1989, chemists Stanley Pons and Martin Fleischmann excited the world with claims that they had produced fusion at room temperature — "cold" fusion compared to the high temperatures the process was thought to require. Their discovery seemed to offer a potential solution to the energy crisis: cheap energy, without pollutants or radioactive waste.

Science cannot be absolutely defined: However, scientific endeavors have a set of key characteristics, summarized in the Science Checklist.



theoretical ecology
notes from ecology, biogeography and evolution by Florian Hartig

Home | RSS feed | Twitter @TheorEcology | Ecology jobs

Statistical analysis with blinded data — a way to go for ecology?

Florian Hartig | 04 Feb 2016

In the last post about the Higgs rumors, I referred to an excellent blog post by Matt Stricker that features a long comment exchange between him and Peter Woit about the implications for using information about the experimental results before the data analysis has been completed. One thing that made me thinking was Matt's point about "blinding the data". From the context, I could understand what they referred to, but confirming my intuition on Wikipeda made the aware how common such a blinded analysis seems to be in particle physics. From the article about blind experiments.

Meet the soft, cuddly robots of the future. Rigid robots step aside - a new generation of squishy, stretchy machines is wiggling our way.

“But I don’t handle sensitive data....”

- Security is more than confidentiality; the **integrity** and **availability** of data and instruments is critical for science.
- **Confidentiality** before “going public” with big news.
- **Valuable** data and powerful IT.
- **Everyone is a target**... “internet noise”; ransomware; and open science is... open!
- **Threats?** More than criminals and rivals... environmental risks; lax management.

“Isn’t this just an IT problem?”

Sadly, you cannot plug in and switch on a “solution” for information security.

Information security is about policy, procedures, technology, and people... and if you’re lucky, laws and regulations, too!

Policies provide the framework; procedures and technology can help implement the policy, but **it really comes down to the people to understand/implement the concepts.**

Information Security has a positive impact on the science even for smaller projects -- *it promotes best practices for IT!*

-3-

Cybersecurity Programs

So, what is a cybersecurity “program?”

A cybersecurity program is a **structured approach** to **develop, implement, and maintain** an environment conducive to appropriate levels of information security and risk to the organization’s mission [**i.e., your science mission**].

Cybersecurity programs are made up of **ongoing activities and projects** in the areas of: policies and procedures; controls and mitigations; control verification and assessment; threat monitoring and activity analysis; incident response and remediation; and training and awareness.

Cybersecurity programs should be **scoped** to the key assets, resources, and lifespan of organizations.

Bottom line:

*Security
programs
are living,
breathing
things.*



What does a PI or Project Manager want out of the cybersecurity program?

Enhance the science productivity by:

- Ensuring the availability of key information systems and processes that are critical to the science mission
- Guaranteeing the integrity of the data from accidental or malicious modification
- Protecting the confidentiality of private or sensitive information from accidental or malicious disclosure
- Obtaining these results while minimizing inconveniences and cost of the program

For more information ...

trustedci.org/guide

and see also:

trustedci.org/ctsc-email-lists

trustedci.org/webinars

trustedci.org/useful-links

trustedci.org/trainingmaterials

Advantages of Cybersecurity From Day 0

- Least expensive, most effective.
- Make security a consideration of equipment, software, and service purchases.
- Get data storage/transport right so that you don't have to worry about trying to find/inventory later and wonder what was missed, mishandled, or stored outside project control.
- Avoid disturbing scientists' workflows in the course of retrofitting security measures after tech is in place.

-4-

Programmatic Must-Do's

Must-Do's

1. Classify and inventory data and information flows
2. Identify stakeholders
3. Identify roles and responsibilities
4. Develop core policies / procedures
5. Plan for and determine ownership of:
 - a. Authentication and access controls
 - b. Configuration and vulnerability management
 - c. Monitoring (logs and network activity)
 - d. Incident response and remediation
 - e. Data recovery and retention
 - f. Staff training and user awareness

1 Classification and Inventory

You can't secure what you can't identify and find.

- A. Develop data classification scheme
 - a. No more than 3-4 categories (public, private, sensitive)
 - b. Define rules for data location and protection level
- B. Identify critical systems; work with owners
 - a. Data flows help identify critical information systems
 - b. Based on criticality to project and compliance req'ts
 - c. Availability and integrity are also important issues
- C. Inventory the assets
 - a. List assets and categorize by type and level of protection
 - b. Develop in consultation with system owners
 - c. Helps with cybersecurity resource allocation

2 Identify Stakeholders

- **Project leadership.** Involvement is essential.
- **Institutions.** Have requirements or provide resources
- **Data subjects / research participants.** Obligations?
- **Funding agency.** Involvement? Resources?

3 Identify Roles & Responsibilities

- **Project leadership.** Budget and set priorities for security, accept risk on behalf of the project, ultimately responsible for security.
- **System owners.** Understand capabilities/implications of systems and their interactions, advise project leadership and implement technical controls.
- **Users / personnel.** Understand how cybersecurity protects the science mission, practice good security hygiene.

4 Policies and Procedures

A little bit of planning can go a long way.

Developing some core policy results in:

- Getting people on the same page, *literally* (including stakeholders, new personnel, students)
- Enriched knowledge about your environment

Master Information Security Policy and Procedures (MISPP)

Purpose: Core, general policies + guide for navigating the full corpus of policies and procedures.

Audience: You and all your stakeholders.

- Roles & Responsibilities (... CISO, Leadership)
- Developing, Implementing, and Maintaining Our Cybersecurity Program (... core processes)
- Resources & Key Contacts (... we're here to help)
- Other Policy and Procedure Documents (... a gateway of sorts)
- Enforcement provisions
- Terms & Acronyms
- *... plus anything else so central to the program that it warrants stating here*

5 Plan for and determine ownership of ongoing operational activities

- Authentication and access controls
- Configuration and vulnerability management
- Monitoring (logs and network activity)
- Incident response and remediation
- Data recovery and retention
- Staff training and user awareness

Understand resources available to you at: <https://protect.iu.edu/>

<http://researchtech.iu.edu/>

Review existing program: <https://protect.iu.edu/online-safety/program/safeguards/>

Questions

Authentication and Authorization

Also referred to as Identity and Access Management (IAM)

Controls access to software and data - who is able to create, read, write, update, or delete

Includes processes for on-boarding and off-boarding

Configuration and Vulnerability Management

Default configurations are normally very insecure

Need to use accepted frameworks for secure initial configurations -- see Security Technical Implementation Guides ([STIG](#)); ensure configuration changes are approved and documented

Vulnerabilities in configuration or software arise on a continual basis -- need to do more than just scan; prioritize remediation

Monitoring

Compromises and intrusion WILL happen

Actively monitoring network traffic and logs can provide early detection

Pay close attention to outbound traffic to unexpected destinations

Incident Response and Remediation

Must have plans in advance for dealing with incidents; practice with table-top exercise

Having a good communication plan is important

Don't be afraid to ask for help -- including institution, peers and law enforcement

Analyze for root cause of failure and repair

Data Recovery and Retention

Backups are essential to limit impact of data loss

Periodic testing data recovery process is essential for it to work when needed

Data retention policies and procedures can limit exposure in legal discovery cases

Staff Training and User Awareness

Everyone must be aware of key policies

Staff must understand procedures and processes and implement them

Users should be aware of the most recent forms of attack

Periodic training is necessary to remind and update



CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

 [@TrustedCI](https://twitter.com/TrustedCI)

We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author(s) and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the National Science Foundation, Indiana University and its offices UIISO or PSIA .